"Importancia de contar con un servicio de sellado digital de tiempo en una PKI"

Javier Díaz, Nicolás Macia, Lía Molinari, Paula Venosa, Alejandro Sabolansky

LINTI, Laboratorio de Investigación en Nuevas Tecnologías Informáticas, Facultad de Informática, Universidad Nacional de La Plata, calle 50 y 120, La Plata, Buenos Aires, Argentina
{javierd, nmacia, lmolinari, pvenosa, nmacia, asabolansky}@info.unlp.edu.ar

Resumen

El tiempo es una magnitud que afecta a todas las actividades humanas y es un componente esencial en todos los procesos. Registrar el momento exacto en que se suceden los acontecimientos es fundamental. Una aplicación que utiliza firma digital sobre una infraestructura PKI[1] exige que la medida de tiempo usada sea precisa y acordada.

El sellado de tiempo (Timestamping) es un mecanismo que permite demostrar que una serie de datos han existido y no han sido alterados desde un instante específico en el tiempo.
El uso de un sistema de sellado de tiempo aparece como indispensable para mantener la validez de los documentos a lo largo de los años.

Contar con un servicio de sellado de tiempo resulta de vital importancia cuando se implementan mecanismos de seguridad y auditoría. El tiempo en que ocurren los eventos es un dato crítico para evaluar si la información es confiable, para correlacionar eventos de seguridad, o para conocer el momento exacto en que se llevó a cabo una acción específica en un sistema, entre otros.

Palabras claves: timestamping, PKI, firma digital, NTP

Contexto

El siguiente trabajo trata sobre el aporte que significa integrar el servicio de sellado digital de tiempo a un proyecto de PKI.

La línea de investigación presentada está inserta en el proyecto de incentivos del LINTI "Redes, Seguridad y Desarrollo de Aplicaciones para e-educación, e-salud, e-gobierno y e-inclusión".

PKIUNLPGRID es la infraestructura que soporta las actividades de e-ciencia de la comunidad académica Argentina. Esta Autoridad de Certificación está acreditada por TAGPMA y el IGTF. La misma es utilizada en los proyectos EELA [1http://www.eu-eela.org/first-phase.php] y EELA 2 [http://www.eu-eela.eu/].

1. Introducción

Al momento de visualizar un documento digital surgen básicamente dos interrogantes

- ¿Quién es el autor de este documento? ¿Quién autorizó su publicación?
- ¿Cuándo fue creado o modificado por última vez dicho documento?

En ambos casos, la pregunta es específicamente sobre ese documento y no otro. Una respuesta al primer planteo permite conocer quién y qué: Quién aprobó exactamente qué en dicho documento.

1 Infraestuctura de clave pública

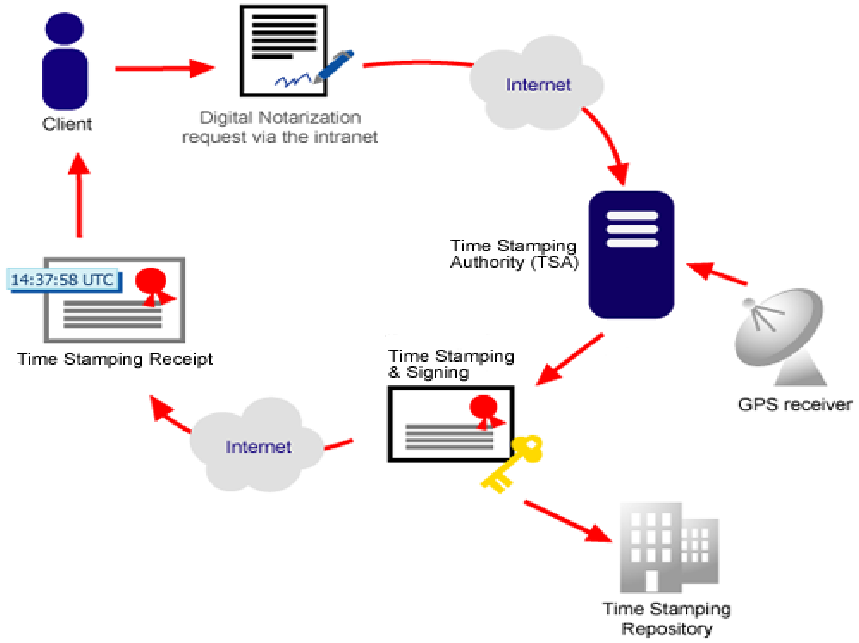
La respuesta a la segunda de las preguntas planteadas permite saber cuándo y qué: Desde cuándo el contenido de ese documento existe.

Las preguntas planteadas ameritan analizar diferentes alternativas. Una alternativa para responder la primera cuestión es la firma digital, mientras que una alternativa para responder la segunda es el sistema de sellado digital de tiempo. En este marco, debe haber un procedimiento con el cual un autor de un documento pueda firmar un conjunto de bytes que actúan como firma. Por otra parte, debe haber un mecanismo de verificación mediante el cual cualquier usuario puede chequear un documento y la firma adjunta para que, con garantía razonable, se pueda asegurar que la misma responde a las preguntas quién y qué o cuándo y qué.
La firma digital es un mecanismo orientado a garantizar la identidad del emisor de la información, a que la misma no se manipule durante la transmisión, a que sea confiable y a que no se pueda repudiar a ninguno de los integrantes de la comunicación.

Esta es la forma que garantiza conocer quién ha hecho qué. Pero hay un parámetro importante que la firma digital no abarca y es el instante de tiempo en que ha sucedido ese determinado suceso. Esta falencia es la que genera el surgimiento de los mecanismos de sellado digital de tiempo.

Características del sellado de tiempo

El servicio de Time Stamping se sustenta en los mecanismos de firma digital y generalmente es un servicio adicional que prestan las autoridades de certificación. A grandes rasgos, existe una tercera parte de confianza, que es aceptada tanto por el emisor como por el receptor, que es la que da fe de la fecha y hora de una transacción. Es decir, añade el dato "tiempo" a la transacción o al documento, por el cual las partes aceptan la validez temporal que se asocia a ese dato determinado.



Fuente: Macao Post eSignTrust

Entidades intervinientes:

La normativa existente [RFC 3161][ISO 18014][X.995] relacionada con el sellado digital de tiempo, distingue las siguientes entidades principales:

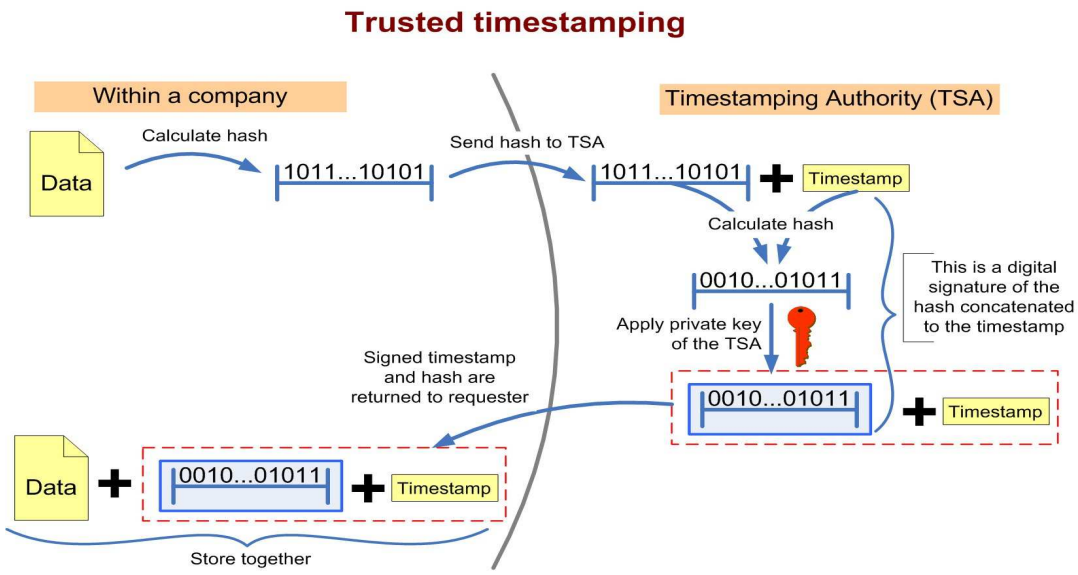
***Solicitante**:*
Es la entidad que posee documentos, información o, en general, cualquier tipo de datos electrónicos a los que quiere incluir un sello de tiempo que garantice que fueron creados previo a la solicitud del sello.
***Verificador**:*
Es la entidad que quiere comprobar que los datos sellados que ha recibido contienen un sello de tiempo válido. Incluso podría ser la misma entidad que utilizó el servicio de sellado de tiempo, para comprobar que el sello generado es válido y correcto.
Autoridad de sellado de tiempo:
La autoridad de sellado de tiempo, TSA (Time Stamping Authority, por sus siglas en inglés) es el proveedor del servicio. Su finalidad es la de comprobar la existencia de los datos a sellar y generar el sello de tiempo que irá unido a esos datos. De esta forma, la TSA asegura que esos datos existían en un determinado instante de tiempo y garantiza que el parámetro de tiempo de ese sello es correcto.

Fases de sellado de tiempo

En el sellado de tiempo se diferencian dos procedimientos principales:

***Creación del sello de tiempo**:*
En primer término, el solicitante genera un hash (función o método para generar claves que representen de manera unívoca a un dato) de la información que quiere sellar. Este hash es enviado a la autoridad de sellado de tiempo, la cual anexa el sello de tiempo tiempo al hash y vuelve a calcular el resumen considerando ahora el nuevo dato generado. Este hash es firmado digitalmente con la clave privada de la TSA. Por último el hash firmado junto con el sello de tiempo son enviados al solicitante del sellado de tiempo.
Verificación de sello de tiempo:
Cualquier entidad que confíe en el emisor del sello de tiempo puede verificar que el documento no fue creado después de la fecha que indica el sello. Para probar esto, se calcula el hash de la información original, se concatena a este hash el sello de tiempo recibido y se vuelve a calcular una nueva función de hash.
En este punto, resta validar la firma digital de la TSA. Se debe verificar que el hash recibido fue firmado con la clave privada. Para ello, se aplica la clave pública de la TSA a dicho dato, y se comparan ambos hash. Esta comprobación permite probar que el sello de tiempo y el mensaje no fueron alterados y que efectivamente fue emitido por la autoridad de sellado .

Proceso de solicitud de sellado de tiempo. Fuente: Wikipedia



2. Líneas de investigación y Desarrollo

El sellado digital de tiempo tiene aplicación en una gran cantidad de actividades, entre las que se destacan la facturación electrónica, las transacciones seguras en comercio electrónico, los registros electrónicos, la trazabilidad de operaciones, donde el instante de tiempo en que transcurre cada una de las operaciones inherentes a las mismas es un valor que debe ser preciso y confiable.

La integración de este servicio a un servicio de certificación de firma digital, brinda un respaldo a las actividades mencionadas, pudiendo utilizar este sello como elemento de prueba ante situaciones en las que se deba demostrar la existencia de un hecho determinado.

Para citar un ejemplo de la importancia de la certificación del tiempo en operaciones financieras, directivos de la empresa bursátil estadounidense Rite-Aid [SEC], antedataron cartas de garantía de compensaciones para enriquecerse en millones de dolares, y posteriormente intentaron eliminar las pruebas deshaciéndose del equipamiento utilizado para alterar las fechas.

3. Resultados obtenidos/esperados

A fin de implementar la infraestructura sobre la cual se va a montar la autoridad de sellado de tiempo se han estudiado y analizado los requisitos del servicio, teniendo en cuenta la normativa vigente y las distintas alternativas para cada uno de los componentes. También se ha definido la política de sellado digital de tiempo [RFC 3628] adecuándose a lo especificado en la política de la autoridad de certificación y siguiendo las recomendaciones de las normativas existentes [TS 101861].

Como fuente confiable de tiempo a ser consultada por la TSA para sellar los requerimientos, se ha optado por usar el protocolo NTP[2][RFC 1305] (teniendo en cuenta que e un protocolo estándar muy aceptado), utilizando como fuente de referencia distintas referencias las cuales proveen redundancia puesto que se alcanzan tanto por Internet como por Internet2. Además se cuenta en la UNLP con un reloj propio tipo GPS[3].

Hoy en día se están analizando y evaluando herramientas para implementar el servicio de sellado de tiempo con productos opensource e integrarlo al servicio de certificados digitales PKIUNLPGRID [https://www.pkigrid.unlp.edu.ar] en la UNLP en los próximos meses. Esta integración permitirá que aplicaciones que se implementen en el futuro y utilicen firma digital, cuenten además con el servicio de sellado de tiempo que permitirá a la aplicación garantizar la existencia de los datos previo a una fecha determinada.

En el momento de la implementación se planea considerar la puesta en marcha de servidores redundantes de almacenamiento, donde se resguardarán los sellos de tiempo emitidos para su posterior consulta y servidores replicados para poder recibir las solicitudes de los sellos de tiempo.

2 NTP: Network Time Protocol. Protocolo de Internet para sincronizar los relojes, estandarizado por la IETF como RFC 1305.

3 GPS: sistema de posicionamiento mundial

Además se deberán definir mecanismos de seguridad y monitoreo de todos los componentes implementados con el fin de brindar un servicio 7X24.

4. Formación de recursos humanos

Desde hace varios años, un grupo de integrantes del LINTI desarrolla su labor de investigación en el área de seguridad y auditoría. En el área de seguridad, una de las líneas de investigación que se ha desarrollado es la vinculada a Infraestructura de Clave Pública y Firma Digital. En esa línea se han realizado varias tesis de grado, entre ellas "Utilizando firma digital: montando una PKI que utiliza firma digital como soporte de las distintas instancias de un sistema administrativo" (Lic. Fredes y Lic Venosa), "Integración de aplicaciones/servicios basados en Web usando firma digital" (Lic. Romero y Lic. Fonseca) e "Implementando Firma Digital con J2EE" (Lic. Falcone y Lic. Clemens). En esta línea, actualmente el Proyecto PKIUNLPGrid en el cual trabajan 5 integrantes del LINTI, logró acreditar en el año 2007 una Infraestructura de certificados digitales para los proyectos EELA y EELA 2. La autoridad de certificación reconocida internacionalmente, actualmente está operativa, brindando servicios a la comunidad académica involucrada en proyectos de e-ciencia.

Además se han escrito artículos en diversos congresos. En 2009 se ha presentado en las jornadas chilenas de computación un artículo que plantea la implementación de múltiples autoridades de registro en PKIUNLPGrid. En ese marco se realizó también en 2009 un taller para Autoridades de Registro y operadores, a fin de capacitar a los mismos y de posibilitar su incorporación a la Infraestructura existente.

En esta línea de trabajo, se está investigando el aporte de servicios de sellado digital de tiempo en una infraestructura de PKI. En ese marco, actualmente se encuentra en desarrollo la tesis de grado de la carrera de Licenciatura en Informática de la Universidad Nacional de La Plata del alumno Alejandro Javier Sabolansky.

5. Bibliografía

- [RFC 3628] Adams, P., Pinkas, Bull, N. Pope, J. Ross, "Policy Requirements for Time-Stamping Authorities (TSAs)", RFC 36128, November 2003.
- [TS 101861] ETSI Technical Specification TS 101 861 V1.2.1. (2001-11). Time stamping profile. Note: copies of ETSI TS 101 861 can be freely downloaded from the ETSI web site www.etsi.org.
- [X9.95] American National Standard X9.95-2005. Trusted Time Stamps, Accredited Standards Committee X9, www.x9.org, March 2005
- [ISO 18014] ISO/IEC 18014 Information Technology – Security Techniques – Time Stamping Services, ISO/IEC Joint Technical Committee One (JTC1), 2003
- [RFC 3161] Adams, C., Cain, P., Pinkas, D. and R. Zuccherato, "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)", RFC 3161, August 2001.
- [SEC] http://www.sec.gov/news/press/2002-92.htm
- [RFC 1305] David Mills, "Network Time Protocol (Version 3) Specification, Impl", RFC 1305, March 1992.